UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/761,410	01/22/2004	Yuji Handa	0038-0424P	3321

2292 7590 05/16/2007
BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER	
TURCHEN, JAMES R	
ART UNIT	**PAPER NUMBER**
2139	

NOTIFICATION DATE	DELIVERY MODE
05/16/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mailroom@bskb.com

Office Action Summary	Application No.	Applicant(s)	
	10/761,410	HANDA ET AL.	
	Examiner	Art Unit	
	James Turchen	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *THREE* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 January 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *01/22/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-8 are pending.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 5-8 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Hush functions and hush values are not well known in art at the time of invention. In addition, the specification does not enable one of ordinary skill in the art to make and use a hush function or hush value.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1 and 2 are rejected under 35 U.S.C. 102(b) as being anticipated by Harrison (US 5,870,468).

Regarding claim 1:

Harrison discloses a data recording apparatus, comprising:

means for determining a password (column 3 lines12-13, the user inputs a secret key (password) to be used in the encryption and decryption steps);

means for storing data (column 4 lines 11-15, hard disk 30);

means for encrypting the stored data on the basis of the password inputted (column 3 lines 16-21, a scrambled encryption key is made from the secret key and it is inherent the program will not continue until the secret key is entered; column 4 lines 11-15, the file are encrypted using the encryption key);

means for writing the encrypted data on a recording medium (column 4 lines11-15, file protection agent 12 reads the file, encrypts it, and writes it back to hard disk 30); and

means for controlling said determining means (column 3 line 53, initialization program gets input from user for secret key) , said storing means, said encrypting means and said writing means (column 4 lines 11-15, File Protection Agent 12 controls reading, encrypting, and writing).

Regarding claim 2:

Harrison discloses a data reading apparatus, comprising:

means for inputting a password, which has been previously determined (column 4 lines 35-39, a screen saver requires the secret key to be entered);

means for reading encrypted data from a recording medium (column 5 lines 15-17, file protection agent 12 reads the target file to be decrypted);

means for decrypting the encrypted data on the basis of the password (column 4 lines 39-41, the scrambled encryption key is recovered by using the inputted secret key; column 5 lines 15-17, decrypts the scrambled file with the encryption key); and

means for controlling said inputting means (column 4 lines 30-59, file protection agent 12 requires the correct password to be input), said reading means and said decrypting means (column 5 lines 15-17, file protection agent 12 reads and decrypts the file).

Claims 5-8 are rejected under 35 U.S.C. 102(e) as being anticipated by Matyas, Jr. et al. (US 7,010,689; herein Matyas).

Regarding claims 5 and 7:

Matyas discloses data recording apparatus, comprising:

means for determining a password (column 9 lines 6-13, user inputs password (pw), fid may be inputted by the user or generated from the file name (ancillary password));

means for storing data and hush function data (hush is considered by examiner to mean hash hereafter, figure 2, memory 236);

means for encrypting the stored data (column 10 line 5, the file is encrypted using the encryption key);

means for writing the encrypted data on a recording medium (column 10 lines 20-32, stores the data); and

means for controlling said storing means, said determining means, said encrypting means and said writing means (figure 3, processor 238 controls storing means, determining means, encrypting and writing means),

wherein said controlling means converts the password into a hush value on the basis of the hush function data, and said encrypting means encrypts the stored data on the basis of the hush value (column 9 lines 19-35, ke, ki, and hash(ke,ki) are encrypted with k, k being the hash(id,pw,fid)).

Regarding claim 6 and 8:

Matyas discloses a data reading apparatus, comprising:

means for inputting a password, which has been previously determined (column 11 lines 17-20, user enters password; fid may be inputted by the user or generated from the file name (ancillary password));

means for storing hush function data (figure 2, memory 236);

means for reading encrypted data from a recording medium (column 11 lines 43-46, the file server returns file header and the encrypted file);

means for decrypting the encrypted data (column 11 lines 50-62, k is used to decrypt ke and ke is used to decrypt the file); and

means for controlling said inputting means, said storing means, said reading means and said decrypting means (figure 3, processor 238 controls storing means, determining means, encrypting and writing means),

wherein said controlling means converts the password into a hush value on the basis of the hush function data, and said decrypting means decrypts the encrypted data

on the basis of the hush value (column 11 lines 49-55, k=Hash(id, pw, fid) and k is used to decrypt ke, ki, and Hash(ke,ki)).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 3 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Harrison as applied to claims 1 and 2 above, and further in view of Matyas, Jr et al. (US 7,010,689; herein Matyas).

Regarding claim 3:

Harrison discloses the data recording apparatus according to claim 1,

wherein an ancillary password is previously stored in said storing means (column 2 lines 61-62, at the initial time an encryption key is generated; column 4 lines 1-4, encryption key is stored in RAM),

Harrison does not disclose said controlling means adds the ancillary password to the password inputted, and said encrypting means encrypts the stored data on the basis of the combined password.

Matyas discloses said controlling means adds the ancillary password to the password inputted (column 9 lines 6-21, the user submits userid, password, and a unique fileid; a hash is computed of the fileid (ancillary password) and the inputted password), and said encrypting means encrypts the stored data on the basis of the combined password (column 9 line 35, shows encrypting data using the combined password k).

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the encryption key of Harrison by hashing the encryption key with the inputted password in order to further complicate reproduction of the encryption key and password.

Regarding claim 4:

Harrison discloses the data reading apparatus according to claim 2,

further comprising means for storing an ancillary password (column 4 lines 39-43, encryption key is stored on the hard disk),

Harrison does not disclose wherein said controlling means adds the ancillary password to the password inputted, and said decrypting means decrypts the encrypted data on the basis of the combined password.

Matyas discloses controlling means adds the ancillary password to the password inputted (column 11 line 49, k=Hash(id, pw (password), fid (ancillary password), and decrypting means decrypts the encrypted data on the basis of the combined password (column 11 lines 50-54, k is used to decrypt and recover the data).

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the encryption key of Harrsion by hashing the encryption key with the inputted password in order to further complicate reproduction of the encryption key and password.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Prior art discloses key encrypting keys and file encryption schemes.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Turchen whose telephone number is 571-270-1378. The examiner can normally be reached on MTWRF 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JRT

TAGHI ARANI
PRIMARY EXAMINER
5/10/07